|  |  |  |
| --- | --- | --- |
| Name: Adarsh Kumar | SRN No: PES2UG20CS016 | Assignment No:06 |
| Section: B | Date: 15/10/2022 |

|  |  |
| --- | --- |
|  | **Verification of the DNS setup** |
| Screenshots | Get the IP address of ns.attacker32.com  Command: dig ns.attacker32.com    We can see that the answer section has name ns.attacker32.com and the IP address of that name server is 10.9.0.1553  Get the IP address of [www.example.com](http://www.example.com)  Command: dig www.example.com  dig @ns.attacker32.com [www.example.com](http://www.example.com)    This is an authentic server and it’s IP address is 93.184.216.34    This a proxy server which is created by attack and it’s IP address is 1.2.3.5  Verifying with the cache in local DNS server |
| Task 1: | Construct DNS request |
| Attacker Terminal |  |
| Wireshark | In the above Wireshark short we can observer that in flag section it shows that there is no such name exist as per the name server of icann. |
| Task 2: | Spoof DNS Replies |
| Screenshot | Finding the IP addresses of the name servers of the example.com domain  As we can see that ns command gave us two name servers in Answer Section  and we use dig +short command to get the IP address of those two server names.  a.iana-server.net    b.iana-server.net |
| Wireshark | Server : a.iana-server.net    Server : b.iana-server.net    In the answer section of both packets we can see that we are getting the spoofed reply 1.2.3.4 |
| Task 3: | Launch the Kaminsky Attack |
| Attacker screenshot | Attack done using C and python in hybrid mode so that our attack becomes fast  We can see that a lot fake DNS response is being sent to the network |
| Cache Screenshot | As we can see in that cache that name server of the example.com domain is replaced attacker32.com hence attack successful  We can also see that a lot of random entry in the cache are there |
| Task 4: | Result Verification |
| User screenshot | On the victim terminal run the command:  # dig www.example.com    # dig @ns.attacker32.com [www.example.com](http://www.example.com)    Here we can observer that both [www.example.com](http://www.example.com) and @ns.attacker32.com [www.example.com](http://www.example.com)  Have same IP address so that implies our attack on remote DNS is successful. |
| Wireshark | Observe that response contains attackers name server to get the IP of the host name example.com |